BURSOR & FISHER, P.A.
L Timothy Fisher (State Bar No. 191626)
Joel D. Smith (State Bar No. 244902)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
jsmith@bursor.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

AUDRA GRAHAM and STACY MOISE, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

NOOM INC. and FULLSTORY, INC.,

Defendants.

Case No. 3:20-cv-06903-LB

PLAINTIFFS' OPPOSITION TO FULLSTORY'S MOTION TO DISMISS THE FIRST AMENDED COMPLAINT

Date: Apr. 8, 2021
Time: 9:30 a.m.
Courtroom: B, 15th Floor
Judge: Hon. Laurel Beeler

TABLE OF CONTENTS

PAGE(S)

INTRODUCTION 1

ARGUMENT 2

I. THE COURT HAS SPECIFIC PERSONAL JURISDICTION OVER FULLSTORY 2

A. The Purposeful Direction Requirement Is Satisfied 3

1. Wiretapping And Internet-Tort Cases Support The Purposeful Direction Requirement Here 3

(i) The First Prong of the Effects Test Is Satisfied 3

(ii) The Second and Third Prongs of the Effects Test Are Satisifed 3

2. FullStory's Authorities Do Not Support Dismissal 6

B. The Claims Arise Out of Forum-Related Activities 8

C. The Exercise of Jurisdiction Is Reasonable 8

II. PLAINTIFFS SUFFICIENTLY ALLEGE A CLAIM UNDER § 631(a) 10

A. FullStory Was Not A Party To The Communication 10

1. FullStory's Arguments Contradict The Pleadings 10

2. FullStory's Arguments Contradict The Text Of The Statute And Relevant Caselaw 10

3. None Of FullStory's Authorities Support Its Position 12

4. FullStory's Contention That Liability Here Would "Criminalize" The Internet Does Not Support Dismissal 13

B. Plaintiffs' Website Interactions Are "Communications" Under *Moosejaw*, *In re Facebook*, and *In re Zynga* 13

C. Noom's Privacy Policy Does Not Support Dismissal 16

1. Plaintiffs Were Wiretapped Before The Hyperlink To The Privacy Policy Appeared On Plaintiffs' Screens 16

2. The Privacy Policy Arguments Fail Under *Nguyen* 17

3. The Privacy Policy Does Not Disclose The Wiretapping 18

III. PLAINTIFFS SUFFICIENTLY ALLEGE A CLAIM UNDER § 635 21

A. Plaintiffs Have Both A Private Right Of Action And Standing To Assert A Claim Under § 635 21

B. Fullstory's Code Is A "Device" That Is "Primarily Or Exclusively" Designed For Eavesdropping 23

IV. PLAINTIFFS STATE A CLAIM FOR INVASION OF PRIVACY 24

CONCLUSION 25

TABLE OF AUTHORITIES

PAGE(S)

CASES

Bergstein v. Parmar,
2014 WL 12586073 (C.D. Cal. June 23, 2014) ..... Passim

Berman v. Freedom Financial Network, LLC,
2020 WL 5210912 (N.D. Cal. Sept. 1, 2020) 18

Boschetto v. Hansing,
539 F.3d 1011 (9th Cir. 2008) 7

Campbell v. Facebook Inc.,
77 F. Supp. 3d 836 (N.D. Cal. 2014) 13, 20, 24

Carson v. Verismart Software,
2012 WL 1038713 (N.D. Cal. Mar. 27, 2012) 9

Colgate v. JUUL Labs, Inc.,
402 F. Supp. 3d 728 (N.D. Cal. 2019) 17, 18

Cothron v. White Castle Sys., Inc.,
467 F. Supp. 3d 604 (N.D. Ill. 2020) 16

CrossFit, Inc. v. Fitness Trade sp. z o.o.,
2020 WL 6449155 (S.D. Cal. Nov. 2, 2020) 4, 5

Francis v. Api Tech. Servs., LLC,
2014 WL 11462447 (E.D. Tex. Apr. 29, 2014) 8, 9

Freestream Aircraft (Bermuda) Ltd. v. Aero Law Grp.,
905 F.3d 597 (9th Cir. 2018) 4, 7

Gadda v. State Bar of Cal.,
511 F.3d 933 (9th Cir. 2007) 9, 18

Good Job Games Bilism Yazilim Ve Pazarlama A.S. v. SayGames LLC,
458 F. Supp. 3d 1202 (N.D. Cal. 2020) 5

Goodman v. HTC Am., Inc.,
2012 WL 2412070 (W.D. Wash. June 26, 2012) 24

Hernandez v. Williams, Zinman & Parham PC,
829 F.3d 1068 (9th Cir. 2016) 11

In re Carrier IQ, Inc.,
78 F. Supp. 3d 1051 (N.D. Cal. 2015) 23

In re Facebook Internet Tracking Litig.,
263 F. Supp. 3d 836 (N.D. Cal. 2017) 23

In re Facebook, Inc. Internet Tracking Litig.,
956 F.3d 589 (9th Cir. 2020) ..... Passim

In re Google Inc. Cookie Placement Consumer Privacy Litigation,
806 F.3d 125 (3d Cir. 2015) 25

In re Google Inc.,
2013 WL 5423918 (N.D. Cal. Sept. 26, 2013) 17, 20, 21

In re Pharmatrak, Inc.,
329 F.3d 9 (1st Cir. 2003) 14

In re Vizio, Inc. Consumer Privacy Litig.,
238 F. Supp. 3d 1204 (C.D. Cal. 2017) 25

In re Zynga Privacy Litig.,
750 F.3d 1098 (9th Cir. 2014) 1, 14, 15

Ion Equip. Corp. v. Nelson,
110 Cal. App. 3d 868 (1980) 22

Kauders v. Uber Techs., Inc.,
2019 WL 510568 (Mass. Super. Ct. Jan. 3, 2019) 16

Koala v. Khosla,
931 F.3d 887 (9th Cir. 2019) 15

LiveCareer Ltd. v. Su Jia Techs., Ltd.,
2015 WL 1448505 (N.D. Cal. Mar. 31, 2015) 6

Loomis v. Slendertone Distribution, Inc.,
420 F. Supp. 3d 1046 (S.D. Cal. 2019) 5

Luis v. Zang,
833 F.3d 619 (6th Cir. 2016) 22

Maree v. Deutsche Lufthansa AG,
2021 WL 267853 (C.D. Cal. Jan. 26, 2021) 18

Mastronardo v. Mastronardo,
2018 WL 495246 (Pa. Super. Ct. Jan. 22, 2018) 17

Mavrix Photo, Inc. v. Brand Techs., Inc.,
647 F.3d 1218 (9th Cir. 2011) ..... Passim

McCoy v. Alphabet, Inc.,
2021 WL 405816 (N.D. Cal. Feb. 2, 2021) 19, 20, 21

Membrila v. Receivables Performance Mgmt.,
2010 WL 1407274 (S.D. Cal. Apr. 6, 2010) 12

Menken v. Emm,
503 F.3d 1050 (9th Cir. 2007) 10

Moreno v. San Francisco Bay Area Rapid Trans. Dist.,
2017 WL 6387764 (N.D. Cal. Dec. 14, 2017) 17

Motley v. ContextLogic, Inc.,
2018 WL 5906079 (N.D. Cal. Nov. 9, 2018) 18

Myers v. Bennett Law Offices,
238 F.3d 1068 (9th Cir. 2001) 4

Nguyen v. Barnes & Noble Inc.,
763 F.3d 1171 (9th Cir. 2014) 1, 17, 18

Oakley, Inc. v. Donofrio,
2013 WL 12126017 (C.D. Cal. June 14, 2013) 5

Opperman v. Path, Inc.,
205 F. Supp. 3d 1064 (N.D. Cal. 2016) 17, 19, 20, 25

Panavision Int'l, L.P. v. Toeppen,
141 F.3d 1316 (9th Cir. 1998) 10

Picot v. Weston,
780 F.3d 1206 (9th Cir. 2015) 7

Rainsy v. Facebook, Inc.,
311 F. Supp. 3d 1101 (N.D. Cal. 2018) 14

Revitch v. New Moosejaw, LLC,
2019 WL 5485330 (N.D. Cal. Oct. 23, 2019) ..... Passim

Ribas v. Clark,
38 Cal. 3d 355 (1985) 11

Rogers v. Ulrich,
52 Cal. App. 3d 894 (1975) 12

Romero v. Securus Techs., Inc.,
216 F. Supp. 3d 1078 (S.D. Cal. 2016) 22

Roney v. Miller,
705 F. App'x 670 (9th Cir. 2017) 25

S.D. v. Hytto Ltd.,
2019 WL 8333519 (N.D. Cal. May 15, 2019) ..... Passim

Schwarzenegger v. Fred Martin Motor Co.,
374 F.3d 797 (9th Cir. 2004) 2, 6, 9

Sennheiser Elec. Corp. v. Chutkowski,
2012 WL 13012471 (C.D. Cal. Apr. 20, 2012) 7

Spokeo, Inc. v. Robins,
136 S. Ct. 1540 (2016) 22

Stack v. Progressive Select Ins. Co.,
2020 WL 5517300 (N.D. Cal. Sept. 14, 2020) 6

Stomp, Inc. v. NeatO, LLC,
61 F. Supp. 2d 1074 (C.D. Cal. 1999) 5

Sun Grp. U.S.A. Harmony City, Inc. v. CRRC Corp. Ltd.,
2018 WL 10689420 (N.D. Cal. July 9, 2018) 7

United States v. Eady,
648 F. App'x 188 (3rd Cir. 2016) 10

United States v. Clayton,
2020 WL 3034826 (E.D. Pa. June 4, 2020) 17

United States v. Forrester,
512 F.3d 500 (9th Cir. 2008) 14

Valentine v. Nebaud, Inc.,
2009 WL 8186130 (N.D. Cal. Oct. 6, 2009) 3

Walden v. Fiore,
571 U.S. 277 (2014) 6

Ziegler v. Indian River County,
64 F.3d 470 (9th Cir. 1995) 9

STATUTES

18 U.S.C. § 2512(b) 22

Cal. Penal Code § 631 ..... 11, 13, 14, 16

Cal. Penal Code § 635 ..... 21, 22, 23, 24

Cal. Penal Code § 637.2(b) 22

RULES

Fed. R. Civ. P. 9(b) 3

INTRODUCTION

Noom hired FullStory to secretly make recordings of everything anyone does on its website, noom.com, using a tool called "Session Replay." With this tool, Defendants "watch and record a visitor's every move on a website, in real time" with FullStory's software providing "pixel-perfect playback." FAC ¶¶ 20, 22-27. Defendants also can monitor website visitors *live* where (in FullStory's own words) "you'll essentially be riding along in near real time." *Id.* at ¶ 30. This technology is not normal, not safe, and "far exceeds user expectations." *Id*. at ¶ 55; *see also id.* at ¶¶ 28, 34. It also violates California's privacy and wiretap laws. FullStory's motion to dismiss should be denied in its entirety.

First, FullStory—but not Noom—argues this Court lacks specific personal jurisdiction over it.[1] The notion that the Court lacks personal jurisdiction over someone who wiretaps Californians across state lines defies common sense. There are many decisions supporting personal jurisdiction both in the context of wiretapping, and in the context of torts committed over the Internet. FullStory does not cite any case holding that a court lacks specific jurisdiction over a person who wiretaps across state lines, and is apparently asking this Court to be the first to do so.

Second, most of FullStory's arguments concerning the wiretapping claim under CIPA § 631(a) are rebutted by *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019), which involved very similar facts, and several circuit court decisions addressing the monitoring of internet activity, including two in the Ninth Circuit: *In re Facebook, Inc. Internet Tracking Litig*., 956 F.3d 589, 607 (9th Cir. 2020), and *In re Zynga Privacy Litig*., 750 F.3d 1098, 1107 (9th Cir. 2014). FullStory also advances the novel argument that the mere existence of a privacy policy on noom.com—regardless of whether anyone saw it—furnishes a complete defense. Putting aside the fact that the wiretapping began before anyone would have an opportunity to review the privacy policy, FullStory cites no authority for its position, which contradicts the Ninth Circuit's decision in *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171 (9th Cir. 2014).

[1] FullStory also argues the Court lacks general personal jurisdiction over it, but Plaintiffs do not contend general jurisdiction applies here.

Third, FullStory argues Plaintiffs lack standing to sue under CIPA § 635, and that they cannot be liable in any event because the technology is not "primarily or exclusively designed or intended for eavesdropping." These arguments are contradicted by the aforementioned authority and the language of the statute. At best, they involve factual disputes about whether FullStory's software qualifies as a "device" within the meaning of § 635.

Fourth, the question of whether surreptitiously recording website activity is egregious enough to support a common law invasion of privacy claim is a question of fact. *See In re Facebook*, 956 F.3d at 607 ("The ultimate question of whether Facebook's tracking and collection practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage."). Adopting FullStory's arguments for dismissal of the common privacy law claim would be reversible error under *In re Facebook*.

ARGUMENT

I. THE COURT HAS SPECIFIC PERSONAL JURISDICTION OVER FULLSTORY

The first problem with FullStory's jurisdictional arguments is that FullStory jumbles together the "purposeful availment" standard applicable to contract claims with the "purposeful direction" standard applicable to torts, while ignoring factors that do not support FullStory's position. *See* MTD at 6:23 (quoting *Schwarzenegger*'s standard for contract claims, while omitting standard for tort claims stated in the same decision); *id.* at 7:20-24; 8:8-10 (focusing on FullStory's contract with Noom). As the Ninth Circuit held in a decision involving torts on the Internet, the "purposeful direction" standard "is the proper analytical framework" for torts. *Mavrix Photo, Inc. v. Brand Techs., Inc.*, 647 F.3d 1218, 1228 (9th Cir. 2011) ("*Mavrix*"); *see also Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 800 (9th Cir. 2004) ("A purposeful availment analysis is most often used in suits sounding in contract … A purposeful direction analysis, on the other hand, is most often used in suits sounding in tort."). Wiretapping claims are governed by the "purposeful direction" analysis because they sound in tort. *See S.D. v. Hytto Ltd.*, 2019 WL 8333519, at *2 (N.D. Cal. May 15, 2019) ("*Hytto*") (applying purposeful direction test in wiretapping case); *Bergstein v. Parmar*, 2014 WL 12586073, at *3 (C.D. Cal. June 23, 2014) (same).

As set forth below, there are many cases involving wiretapping and Internet-based torts that support the conclusion that the "purposeful direction" requirement is satisfied here, as well as the remaining two requirements for specific personal jurisdiction: forum-related activities and reasonableness.

A. The Purposeful Direction Requirement Is Satisfied

1. Wiretapping And Internet-Tort Cases Support The Purposeful Direction Requirement Here

The "purposeful direction" analysis "focuses on the forum in which the defendant's actions were felt, whether or not the actions themselves occurred within the forum." *Mavrix*, 647 F.3d at 1228 (internal quotation omitted). This analysis requires a three-part "effects test," which turns on whether the defendant "(1) committed an intentional act, (2) expressly aimed at the forum state, (3) causing harm that the defendant knows is likely to be suffered in the forum state." *Id.*

(i) The First Prong of the Effects Test Is Satisfied

At least three courts have held "the 'intentional act' standard is *easily satisfied*" where the plaintiff alleges wiretapping claims. *Hytto*, 2019 WL 8333519, at *4 (emphasis added).[2] Plaintiffs allege FullStory intentionally wiretapped visitors to noom.com. *See* FAC ¶¶ 14-15, 69-70, 80, 88; *see also* Fed. R. Civ. P. 9(b) (intent may be alleged "generally"). FullStory does not address or dispute this factor in its motion. On reply, FullStory will argue that the *only* intentional act it did was to develop software and provide that software to Noom. However, that argument cannot support dismissal because it contradicts the pleadings concerning FullStory's intent. *See* FAC ¶¶ 14-15, 69-70, 80, 88. Further, the clear inference in the FAC that FullStory provided the software to Noom, *so that Defendants could engage in wiretapping. See id.* ¶¶ 1, 19-26, 30, 35-40.

(ii) The Second and Third Prongs of the Effects Test Are Satisifed

As for the second and third prongs of the effects test, FullStory makes an important admission in its brief that supports denial of its motion. Namely, FullStory states, "if the

[2] *See also Bergstein*, 2014 WL 12586073, at *3 ("The 'intentional act' prong is easily satisfied in this case. Parmar committed an intentional act when he allegedly recorded the parties' telephone conversations …."); *Valentine v. Nebaud, Inc.*, 2009 WL 8186130, at *6 (N.D. Cal. Oct. 6, 2009) (holding "the first prong is easily satisfied" in a wiretapping case).

defendant's conduct 'takes place outside the forum,' [as FullStory argues is the case here] there may still be purposeful direction if that conduct has 'effects inside the forum state.'" MTD, 7:18-20 (quoting *Freestream Aircraft (Bermuda) Ltd. v. Aero Law Grp.*, 905 F.3d 597, 604 (9th Cir. 2018)). The effects of wiretapping and other invasion of privacy claims are "felt" where the plaintiff is located. *See Hytto Ltd.*, 2019 WL 8333519, at *2 (wiretapping caused "harm" in the location where plaintiff was located); *Bergstein*, 2014 WL 12586073 at *3, 7 (same); *cf. Myers v. Bennett Law Offices*, 238 F.3d 1068, 1075 (9th Cir. 2001) ("at least one of the 'harms' suffered by [Nevada] Plaintiffs is akin to the tort of invasion of privacy and was felt in Nevada."). FullStory does not deny that the effects of its wiretapping are felt in California.

Even putting FullStory's concession aside, caselaw and the pleadings further support denial of FullStory's motion. The second prong of the "effect test" is satisfied "when a defendant is alleged to have engaged in wrongful conduct targeted at a plaintiff the defendant knows is a resident of the forum state." *Hytto*, 2019 WL 8333519, at *4. Similarly, the third prong is satisfied when the defendant knows the harm "is likely to be suffered in the forum state." *Id.* at *5. There are numerous cases involving wiretapping across state lines, and torts on the Internet, and both lines of cases independently support exercising jurisdiction here. In *Mavrix*, a case involving torts on the Internet, the Ninth Circuit reversed dismissal for the defendant after concluding the defendant "anticipated, desired, and achieved a substantial California viewer base" on a website. *Mavrix*, 647 F.3d at 1230. Hence, under *Mavrix*, courts may exercise personal jurisdiction when a website "with national viewership and scope appeals to, and profits from, an audience in a particular state." *Id.* at 1231; *see also CrossFit, Inc. v. Fitness Trade sp. z o.o.*, 2020 WL 6449155, at *4 (S.D. Cal. Nov. 2, 2020) (explaining the holding in *Mavrix*).

In *Hytto*, 2019 WL 8333519, at *4-5, a putative class action involving wiretapping, Judge White denied a 12(b)(2) motion, citing allegations that the defendant knew that many of the customers it monitored were in the U.S. *See also Bergstein*, 2014 WL 12586073, at *4 (foreseeability that a Californian would be wiretapped supported personal jurisdiction). Likewise, numerous other courts involving torts on the Internet have denied 12(b)(2) motions where, as here, it was foreseeable that Californians would use commercial or highly interactive websites. *See*

Loomis v. Slendertone Distribution, Inc., 420 F. Supp. 3d 1046, 1068-69 (S.D. Cal. 2019) (personal jurisdiction satisfied where defendant's "interactive website" targeted the California market); *Oakley, Inc. v. Donofrio*, 2013 WL 12126017, at *5 (C.D. Cal. June 14, 2013) (denying 12(b)(2) motion where defendants "conducted regular business with California customers using [an online platform] as a conduit," engaged in a "substantial volume of transactions," and were "actively and affirmatively involved in completing transactions with California consumers"); *Stomp, Inc. v. NeatO, LLC*, 61 F. Supp. 2d 1074, 1077-78 (C.D. Cal. 1999) ("NeatO cannot escape jurisdiction by claiming that its contacts with California are merely fortuitous… [because] it is not being haled into a court in some unexpected location where the Internet is not commonly available, but [instead] into a court in California, where a large portion of the world's Internet users presumably reside.").[3]

Noom.com is a commercial website offering diet plans "throughout California" and the United States, and Plaintiffs allege that while they were in California, they visited Noom's website to view its diet offerings. FAC ¶¶ 4-5, 8. Paragraph 15 of the FAC contains lengthy allegations that FullStory knew and foresaw that the wiretapping would impact Californians, because Californians "form a significant portion of Noom's customer base," and because of the size of the California market and economy. FAC ¶ 15. "The Website operates in both English and Spanish, the first and second most common languages spoken by California residents." *Id.* Thus, as in *Mavrix*, 647 F.3d at 1231, this case involves a website "with national viewership and scope [that] appeals to, and profits from, an audience in a particular state." The allegations that FullStory was aware of a significant customer base in California are similar to the allegations that supported jurisdiction in *Hytto*. *Compare* FAC ¶ 15, *with Hytto*, 2019 WL 8333519 at *4-5 ("It was foreseeable that Hytto's alleged interceptions would harm S.D. and other similarly-situated individuals and that at least some of this harm would occur in the U.S.—where Hytto knew no

[3] In contrast, personal jurisdiction may be lacking if there is "no showing that the defendant actually or constructively knew of [a] California-user base." *Good Job Games Bilism Yazilim Ve Pazarlama A.S. v. SayGames LLC*, 458 F. Supp. 3d 1202, 1209 (N.D. Cal. 2020). Commercial websites that primarily target European or Asian markets, for example, might not support personal jurisdiction. *See CrossFit*, 2020 WL 6449155 at *4 (personal jurisdiction lacking where the plaintiff admitted the website was "specifically designed" to market products to European consumers). But that is not the case here.

small number of its customers resided."). These allegations must be accepted as true at this juncture. *See id.* at *2; *see also Stack v. Progressive Select Ins. Co.*, 2020 WL 5517300, at *5 (N.D. Cal. Sept. 14, 2020) (Beeler, J.) ("uncontroverted allegations must be taken as true" on a 12(b)(2) motion) (quoting *Schwarzenegger*, 374 F.3d at 800).

On reply, FullStory will attempt to distinguish the above-cited authorities and downplay the above-quoted allegations by emphasizing that FullStory does not own and operate noom.com. That argument might have merit if Plaintiffs had alleged that FullStory simply sold its software to Noom without any further involvement in the wiretapping itself, but those are not Plaintiffs' allegations. Instead, Plaintiffs specifically allege that FullStory is a service provider, and that the service it provides is wiretapping. *See* FAC, ¶ 11; *see also id.* at ¶ 1, 35-40, 72. As an active participant in wiretapping that occurs 24x7x365 (*see id.* ¶ 44), FullStory cannot legitimately argue that its wiretapping of Californians was a fortuitous and unforeseeable event.

2. FullStory's Authorities Do Not Support Dismissal

FullStory does not cite a single wiretapping or Internet-tort case granting a 12(b)(2) motion. Instead, FullStory primarily relies on *Walden v. Fiore*, 571 U.S. 277 (2014), but *Walden* specifically explained that its decision did *not* apply to internet activity. *See id.* at 290 n.9 ("[T]his case does not present the very different questions whether and how a defendant's virtual 'presence' and conduct translate into 'contacts' with a particular state."); *see also LiveCareer Ltd. v. Su Jia Techs., Ltd.*, 2015 WL 1448505, at *4 (N.D. Cal. Mar. 31, 2015) (rejecting argument that *Walden* supported granting 12(b)(2) motion where a commercial website was involved). In fact, *Walden* supports jurisdiction here because, by FullStory's own account, the crux of *Walden* is that "the *defendant* [must] create[] the necessary contacts with the forum" (MTD at 8:2), and that is exactly what a defendant does when it wiretaps across state lines. *See Hytto*, 2019 WL 8333519 at *3-5; *Bergstein*, 2014 WL 12586073, at *3. Indeed, *Hytto* cited *Walden* three times when determining the court had personal jurisdiction over the wiretapping claims in that case. *See Hytto*, 2019 WL 8333519 at *3-5.

FullStory also cites *Picot v. Weston*, 780 F.3d 1206 (9th Cir. 2015), and *Boschetto v. Hansing*, 539 F.3d 1011 (9th Cir. 2008), but neither decision supports dismissal. *Picot* is an example where the court held there was no personal jurisdiction over a tortious interference with contract claim—not a wiretapping claim. Unlike here, the wrongful conduct occurred without "contacting any person in California, or otherwise reaching out to California," and the injury was "not tethered to California in any meaningful way." *Picot*, 780 F.3d at 1215. That analysis is inapplicable in the context of wiretapping across state lines, which necessarily involves "reaching out to California" and causing harm within California.

Boschetto is even less instructive because it involved a contract dispute and thus applied the "purposeful availment" standard, rather than the standard applicable to torts. *See Boschetto*, 539 F.3d at 1016 ("we have typically analyzed cases that sound primarily in contract—as Boschetto's case does—under a 'purposeful availment' standard"). Moreover, as Judge Otero explained when distinguishing *Boschetto*, "the Ninth Circuit drew a distinction between an eBay seller who conducts a single sale and an eBay seller who uses the site to market and sell inventory. The Ninth Circuit noted that personal jurisdiction would be properly exercised over the latter." *Sennheiser Elec. Corp. v. Chutkowski*, 2012 WL 13012471, at *4 (C.D. Cal. Apr. 20, 2012). The same reasoning applies here because FullStory's wiretapping on noom.com was not a one-time event that fortuitously impacted Californians. *See* FAC ¶¶ 14-15; *see also id.* at ¶¶ 37-40, 43-46.[4]

Furthermore, when citing these decisions, FullStory veers into the standard for contract claims by emphasizing that California is not where it entered into its contract with Noom or developed its software. *See* MTD at 7:21-28; 8:8-10. On reply, FullStory will continue to emphasize that it only entered into one contract with Noom outside of California. None of that matters because the "purposeful direction" analysis for torts "*focuses on the forum in which the defendant's actions were felt*, whether or not the actions themselves occurred within the forum."

[4] FullStory's cites in passing a few other cases for general principles concerning personal jurisdiction. None are particularly instructive because they did not involve wiretapping or torts on the Internet. *See Freestream Aircraft (Bermuda) Ltd. v. Aero Law Grp.*, 905 F.3d 597, 604 (9th Cir. 2018); *Sun Grp. U.S.A. Harmony City, Inc. v. CRRC Corp. Ltd.*, 2018 WL 10689420, at *6 (N.D. Cal. July 9, 2018).

Mavrix, 647 F.3d at 1228 (emphasis added). And, as noted in Section I(A)(1) above, FullStory does not (and cannot legitimately) deny that the effects of wiretapping here are felt in California. The fact that FullStory entered into only one contract with Noom is likewise beside the point because the basis for jurisdiction here is FullStory's wiretapping, not its contract with Noom.

B. The Claims Arise Out of Forum-Related Activities

The question of whether a claim "arises out of or relates to the defendant's forum-related activities" is straightforward in a wiretapping case. In *Hytto*, the district court followed FullStory's own authority, *Walden*, when it explained: "[t]he suit-related conduct most pertinent for the analysis at hand is Hytto's alleged interception of communications to (or from) persons in the U.S." *Hytto*, 2019 WL 8333519, at *5; *see also Francis v. Api Tech. Servs., LLC*, 2014 WL 11462447, at *6 (E.D. Tex. Apr. 29, 2014) ("allegations of hacking" into a personal computer involve "activity that is clearly directed at the forum state"); *Bergstein*, 2014 WL 12586073 at *3 ("forum-related activities" requirement satisfied in wiretapping case). So too here, the pertinent forum-related activities are the alleged interception of communications from California visitors to noom.com. *See* FAC ¶¶ 1, 15, 57.

Citing *Walden*, FullStory argues there are no forum-related activities because "[j]ust as in *Walden*, Plaintiffs would have experienced the same alleged harm by visiting Noom's website and interacting with FullStory's software regardless of the state he was in at the time he visited the website." MTD at 8:28-9:3. Yet *Walden* supports Plaintiffs' position—not FullStory's—for the reasons stated in Section I.A.2 above. Further, the argument that Plaintiffs would have been wiretapped regardless of what state they live in does not support FullStory's position: it just shows that FullStory created contacts with every state by wiretapping on a nationwide basis.

C. The Exercise of Jurisdiction Is Reasonable

FullStory's argument that exercising jurisdiction would be unreasonable should be rejected for three separate reasons. First, FullStory ignores its burden. The Ninth Circuit set forth a seven-

part test for reasonableness. *See Ziegler v. Indian River County*, 64 F.3d 470, 475 (9th Cir. 1995).[5] "No factor is dispositive, but the moving party must address each." *Hytto*, 2019 WL 8333519, at *5 (finding defendant failed to meet its burden where "Hytto does not address any of these factors or explain why exercising specific personal jurisdiction would be unreasonable"); *see also Ziegler*, 64 F.3d at 475 ("All seven factors must be weighed").

Here, FullStory ignores the *Ziegler* factors altogether. FullStory will attempt to cure this defect by arguing in support of the factors for the first time on reply, but that tactic is improper and deprives Plaintiffs an opportunity to respond. This Court has held it "will not entertain arguments made for the first time in a reply brief," and it should apply the same rule here. *Carson v. Verismart Software*, 2012 WL 1038713, at 2 (N.D. Cal. Mar. 27, 2012) (Beeler, J.); *Gadda v. State Bar of Cal.*, 511 F.3d 933, 937 n.2 (9th Cir. 2007) ("It is well established that issues cannot be raised for the first time in a reply brief"). Nor could FullStory simply march through each factor in a cursory fashion on reply: FullStory must "present a compelling case that the exercise of jurisdiction would not be reasonable." *Schwartzenegger*, 374 F.3d at 802.

Second, many courts have held it is reasonable to exercise jurisdiction over wiretapping claims. *See*, *e.g.*, *Hytto*, 2019 WL 8333519 at *5; *Bergstein*, 2014 WL 12586073 at *5-6; *Francis*, 2014 WL 11462447 at *6. FullStory cites no contrary authority.

Third, FullStory's only argument is that if the Court exercises jurisdiction here, then FullStory would be subject to jurisdiction anywhere in the United States. MTD at 9:11-17. This is a burden argument, and it fails for two reasons. First, speculation that some unknown person, at some unknown place and time, might later sue FullStory does not make a "compelling case" against jurisdiction *in this case*. Second, FullStory offers no substantive argument for burden in this case, and in any event, burden rarely supports dismissal under Rule 12(b)(2). *See Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316, 1323 (9th Cir. 1998) ("unless the inconvenience [of litigating

[5] The factors are: "(i) the extent of the defendant's purposeful injection in the forum state, (ii) the burden on the defendant of defending in the forum, (iii) the extent of the conflict with the sovereignty of the defendant's state, (iv) the forum state's interest in adjudicating the dispute, (v) the most efficient judicial resolution of the controversy, (vi) the importance of the forum to the plaintiff's interest in convenient and effective relief, and (vii) the existence of an alternative forum." *Ziegler*, 64 F.3d at 475.

in a forum] is so great as to constitute a deprivation of due process, it will not overcome clear justifications for the exercise of jurisdiction."); *accord Menken v. Emm*, 503 F.3d 1050, 1060 (9th Cir. 2007).

II. PLAINTIFFS SUFFICIENTLY ALLEGE A CLAIM UNDER § 631(a)

A. FullStory Was Not A Party To The Communication

FullStory admits that it was "involv[ed] in facilitating the collection of data regarding Plaintiffs' interactions with Noom's website" (MTD at 11:16), but claims it qualifies as a "party to communication" because Noom employed its services. *See id.* at 10:18 ("Noom used FullStory's SaaS."); 11:10 (arguing FullStory was acting "as Noom's service provider"). These arguments fail for four reasons set forth below.

1. FullStory's Arguments Contradict The Pleadings

In *Hytto*, 2019 WL 8333519 at *7-8, the court rejected the same argument FullStory advances here for the simple reason that "[a]t no point" did the plaintiffs allege they communicated with the defendant. *Id.* Likewise, "[A] defendant does not actually participate in a conversation unless his presence is known to the other participants." *United States v. Eady*, 648 F. App'x 188, 192 (3rd Cir. 2016). Thus, a "'party' is a participant whose presence is known to the other parties contemporaneously with the communication." *Id.*; *see also Lopez v. Apple, Inc.*, Case No. 4:19-cv-04577, ECF No. 65, at 8 (N.D. Cal. Feb. 10, 2021) ("Plaintiffs allege that they did not intend Apple to receive their private communications, but that Apple 'captured' such communications using the software in their devices. That sufficiently alleges interception."). Here, as in *Hytto*, Plaintiffs only allege they communicated with noom.com, and that they were unaware of FullStory's eavesdropping. *See* FAC ¶¶ 4-5 (alleging Plaintiffs were "unaware at the time that [their] keystrokes, mouse clicks, and other electronic communications … were being intercepted in real-time and would be disclosed to FullStory, nor did [they] consent to same."); *see also id.* at ¶ 47 ("Users are never told that their electronic communications are being wiretapped by FullStory").

2. FullStory's Arguments Contradict The Text Of The Statute And Relevant Caselaw

Section 631(a) imposes liability for "*any person*" who "aids, agrees with, employs, or

conspires with" anyone who violates § 631(a). Cal. Penal Code § 631(a) (emphasis added). In *Ribas v. Clark*, 38 Cal. 3d 355, 363 (1985), the California Supreme Court explained § 631 "was designed to protect a person placing or receiving a call from a situation where the person on the other end of the line permits an outsider to tap his telephone *or listen* in on the call." (Emphasis in original). "Allow[ing] third persons to eavesdrop on conversations via extensions would be a clear contradiction of the intent of section 631(a)." *Id.* Similarly, last year, the Ninth Circuit explained in *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020) ("*In re Facebook III*"), that the intent of wiretap laws is to "prevent the acquisition of the contents of a message by an *unauthorized third-party or an unseen auditor*"—like FullStory here. *See also id.* at 598 (explaining similar legislative purposes behind CIPA and the federal Wiretap Act).

FullStory cannot escape liability by arguing that it was employed by Noom to facilitate the wiretapping because the statute expressly imposes liability in that scenario. If adopted, FullStory's position would mean that companies could hire undisclosed third parties to eavesdrop on communications with customers and evade liability by claiming the undisclosed eavesdropper was a "party to the communication." In other words, it would eviscerate aiding and abetting liability under the same scenarios described in *Ribas* and *In re Facebook*. Principles of statutory construction do not permit such an interpretation. *See Hernandez v. Williams, Zinman & Parham PC*, 829 F.3d 1068, 1078 (9th Cir. 2016) ("It is a cardinal principle of statutory construction" that a statute should not be construed to render any provision "superfluous, void, or insignificant").

Moreover, Judge Chhabria correctly rejected the same argument FullStory advances here in *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019) ("*Moosejaw*"), a case involving nearly identical facts and issues. Like here, a website operator (Moosejaw.com) hired a third party (NaviStone) to "eavesdrop[] on [plaintiff's website] communications with Moosejaw." *Moosejaw*, 2019 WL 5485330, at *1. Like here, the third party NaviStone argued it was a party to the communications rather than an eavesdropper. *Id.* at *2. As the *Moosejaw* court explained, "it cannot be that anyone who receives a direct signal escapes liability by becoming a party to the communication. Someone who presses up against a door to listen to a conversation is no less an eavesdropper just because the sound waves from the next room reach his ears directly."

Id. The same reasoning applies here, and the fact that FullStory contracted with Noom to engage in wiretapping does not make it any less of an eavesdropper.

3. None Of FullStory's Authorities Support Its Position

FullStory argues it it's a "party to the communication" because it simply furnished a recording device, like those used in *Rogers v. Ulrich*, 52 Cal. App. 3d 894, 899 (1975), and *Membrila v. Receivables Performance Mgmt.*, 2010 WL 1407274, at *2 (S.D. Cal. Apr. 6, 2010). *See* MTD at 10:16-26; 11:15-24. But neither *Rogers* or *Membrila* involved a third-party eavesdropper: they simply involved one person recording another with a tape recorder. That is not the situation here, and just because FullStory furnished the wiretapping device does not rule out that FullStory *also* participated in the wiretapping. Plaintiffs allege FullStory conducted the wiretapping. *See* FAC ¶¶ 2, 25, 27, 29, 30, 45-47, 69-70.

FullStory also cherry-picks a quote from *In re Facebook III*, 956 F.3d at 607, for the vague proposition that courts must "examine the 'technical context' presented by the communications at issue to determine who the parties to those communications are." With respect, FullStory is taking extreme liberties interpreting this decision. *In re Facebook III* reversed dismissal where (as here) the defendant argued it was a party to the communication, and explained that wiretapping laws apply where (as here) "unauthorized third-party or an unseen auditor" eavesdrops on communications. *In re Facebook III*, 956 F.3d at 608. FullStory cites nothing in *In re Facebook III* suggesting the "party communication" defense could apply to undisclosed third parties acting in concert with a website owner.

In connection with its arguments about *In re Facebook III*, FullStory argues Plaintiffs do not "allege that FullStory sold his data, used it for advertising purposes, or disclosed it to any third party." MTD at 11:8-11; *see id.* 12:8-10. Those allegations are not a required element of the claim. *See* Cal. Penal Code § 631(a). FullStory similarly tries to distinguish this case from *In re Facebook III* by noting the defendant in that case, Facebook, sold personal data to advertisers. MTD at 11:27-12:6. But the Ninth Circuit never cited that fact as the basis for reversing dismissal of the CIPA claim, or any other claim. *See In re Facebook*, 956 F.3d at 601-606.

4. FullStory's Contention That Liability Here Would "Criminalize" The Internet Does Not Support Dismissal

FullStory resorts to hyperbole by claiming liability here would "criminalize" the Internet because FullStory's software is no different than the search function on the Court's website. MTD at 12:15-26. However, Plaintiffs allege that FullStory's software is *not* normal, socially accepted, or safe. FAC ¶¶ 28, 34, 55. FullStory is relying on unsupported factual arguments about its technology that cannot be resolved on the pleadings. *See Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 841 (N.D. Cal. 2014) (defendant's factual assertions about how its technology works cannot support 12(b)(6) motion); *Moosejaw*, 2019 WL 5485330 at *3 (same).

B. Plaintiffs' Website Interactions Are "Communications" Under *Moosejaw*, *In re Facebook*, and *In re Zynga*

FullStory argues the Court should dismiss the § 631(a) claim "at least in part" or "to the extent" Plaintiffs based their claim on the collection of information that was not the "contents" of communications. MTD at 13:15; 13:24. FullStory is correct that automatically generated information such as IP addresses, browser types, and the website user's operating system would generally not be actionable under CIPA, and therefore that information is not intended to be covered by Plaintiffs' claims under § 631(a). However, as shown below, there are other communications at issue that FullStory does not dispute qualify as communications, such as mouse movements, keystrokes, scrolls, and medical and health information. FullStory also misstates the law when it argues that website users' names and addresses do not qualify as content.

First, as noted in Section II.A. above, in *Moosejaw*, 2019 WL 5485330, at *1-2, Judge Chhabria denied a motion to dismiss claims under § 631 where, like here, an online clothing retailer hired a third-party technology company to monitor website visitors' mouse clicks, keystrokes, and other website activities. The *Moosejaw* court held "[plaintiff's] interaction with the Moosejaw website is communication within the meaning of section 631." *Moosejaw*, 2019 WL 5485330, at *1.

The outcome in *Moosejaw* is supported by two Ninth Circuit decisions addressing the federal Wiretap Act and CIPA.[6] Last year, the Ninth Circuit reversed dismissal and held that the collection of website visitors' internet history and search terms supported claims under both CIPA and the federal Wiretap Act, because they "divulge a user's personal interests, queries, and habits on third party websites." *In re Facebook III*, 956 F.3d at 604-606. Even URL addresses may qualify as "content" because they reveal "'the particular document within a website that a person views.'" *Id.* at 605 (quoting *United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008)).

Prior to *In re Facebook*, the Ninth Circuit explained that the First Circuit had "correctly concluded" that "the content of the sign-up information customers provided to pharmaceutical websites, which included their 'names, addresses, telephone numbers, email addresses, dates of birth, genders, insurance statuses, education levels, occupations, medical conditions, medications, and reasons for visiting the particular website,'" were actionable communications under the federal Wiretap Act. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1107 (9th Cir. 2014) ("*In re Zynga*") (quoting *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003)). "[S]earch term[s] or similar communication[s] made by the user" on the internet also qualify as "content." *Id*. at 1109. District courts have found a wide array of communications are covered by the Wiretap Act or CIPA, ranging from Facebook "likes" to remotely activated changes to device settings. *See Rainsy v. Facebook, Inc.*, 311 F. Supp. 3d 1101, 1115 (N.D. Cal. 2018); *Hytto*, 2019 WL 8333519, at *7.

Here, the information captured by FullStory's wiretapping is the same type of information covered by the above-cited authorities. The FAC is based on public admissions by FullStory that it records not only which webpages a user visits, but also everything a user does on those webpages, everything they search for, and all the information they provide. *See* FAC ¶¶ 19-27. Dismissal of the § 631(a) claim would be improper because FullStory does not make any argument for dismissal to the extent the claims are based on monitoring which webpages a user visits or searches for (covered by *In re Facebook*), or a user's general website activity such as mouse clicks, keystrokes, and scrolling (covered by *Moosejaw*).

[6] FullStory states, "[t]he analysis of whether something is the 'contents' of a communication under CIPA is the same as it is under the federal Wiretap Act." MTD at 13:6-8.

Second, FullStory mistakenly cites *In re Zynga* for the proposition that "the name, address, and subscriber number or identity of a subscriber or customer" are not "contents" that can support a claim here. MTD at 15:19-20. That interpretation flatly contradicts the portion of *In re Zynga* explaining that "names, addresses, telephone numbers [etc.]" *are* in fact actionable when provided by website users. *See In re Zynga Privacy Litig.*, 750 F.3d at 1107.

FullStory's position stems from a misunderstanding of the term "record information," which generally does not qualify as "content." *Hytto*, 2019 WL 8333519, at *6. "Record information is typically data *generated automatically* at the sending of the message and is incidental to the use of the communication device." *Id.* (emphasis added). "Unlike record information, content is generated not automatically, but through the intent of the user." *Id.* Thus, for example, if someone types in the body of an email that her name is "Jane Doe," then that information qualifies as "content"; whereas the automatic appearance of her name in the email "From" line might not. *See In re Zynga*, 750 F.3d at 1107 (discussing distinction between information typed in an email messages as opposed to "automatically generated" information, and explaining that name, address, and other information provided by website visitors in form fields are "content").

Here, there are no allegations that the names and addresses of website visitors are automatically generated, and it would be improper on a 12(b)(6) motion to draw such an inference against the Plaintiffs. *See Koala v. Khosla*, 931 F.3d 887, 894 (9th Cir. 2019) (addressing standard on 12(b)(6) motion). It is common experience that website users provide information when purchasing items on the Internet, just like the customers who provided their information on the pharmaceutical website referenced in *In re Zynga*, 750 F.3d at 1107. Even if FullStory is correct that *automatically generated* information about users' IP addresses, geolocation, and browser type qualify as "record information," that is not a basis to dismiss the entire claim given that FullStory does not dispute that website interactions and history, as well as medical and health information qualify as content. *See Hytto*, 2019 WL 8333519, at *7 (declining to dismiss wiretap claim in its entirety because not all information described in the complaint was automatically generated "record information").

C. Noom's Privacy Policy Does Not Support Dismissal

Finally, FullStory claims that Plaintiffs' § 631(a) claim must fail because "the privacy policy for Noom's website explicitly disclosed [the wiretapping] to users like Plaintiff." MTD at 14:8-9. Notably, nowhere in its brief does FullStory explicitly argue that the privacy policy established Plaintiffs' consent to be wiretapped. *See generally* MTD at 14:3-15:19. Instead, FullStory appears to take the position that the *mere existence* of the privacy policy furnishes a safe harbor defense—regardless of whether anyone saw the policy, or how well the policy was hidden, or how vague it may be. FullStory cites no authority for that extreme position because there is none. The text of § 631(a) contains no such safe harbor, and FullStory's argument is foreclosed by Ninth Circuit precedent. As set forth below, FullStory's argument fails for three separate reasons, as would any belated consent arguments FullStory may attempt to raise for the first time on reply.

1. Plaintiffs Were Wiretapped Before The Hyperlink To The Privacy Policy Appeared On Plaintiffs' Screens

As an initial matter, Plaintiffs were not even shown a hyperlink to Noom's Privacy Policy until *after* Plaintiffs were already wiretapped. As Plaintiffs allege, Fullstory's wiretapping "begins *the moment* a user accesses or interacts with the Website." FAC ¶ 44 (emphasis added). Thus, the second a user accesses noom.com, FullStory begins recording the user, before a user could possibly read the Privacy Policy. Further, "when a user begins using Noom's website and providing personal information … the hyperlink to Defendant's Privacy Policy disappears until the end of the form on the Website." *Id.* at ¶ 49. Accordingly, users enter their personal information before (allegedly) being told that they are being recorded.

"Colloquially … consent implies permission given *in advance*." *Cothron v. White Castle System, Inc.*, 2020 WL 3250706, at *6 (N.D. Ill. June 16, 2020) (emphasis added) (finding no consent where White Castle asked plaintiff for consent to share biometric information after such information had already been shared); *see also Kauders v. Uber Techs., Inc.*, 2019 WL 510568, at *5 (Mass. Super. Ct. Jan. 3, 2019) (plaintiff did not consent to arbitration where the terms were not disclosed until after the plaintiff created an account); *Mastronardo v. Mastronardo*, 2018 WL 495246, at *5 (Pa. Super. Ct. Jan. 22, 2018) ("[Appellant] claims that consent obtained after-the-

fact is, nonetheless, consent. It is not."); *United States v. Clayton*, 2020 WL 3034826, at *6 (E.D. Pa. June 4, 2020) ("*post hoc* consent forms are ineffective"). Such *ex post facto* or after-the-fact consent cannot be valid under the plain definition of "consent."

2. The Privacy Policy Arguments Fail Under *Nguyen*

Even when the hyperlink to the Privacy Policy appeared on Plaintiffs' screens, Plaintiffs were not on notice of the hyperlink, let alone given the option to *agree* to the Privacy Policy. "The critical question with respect to implied consent is whether the parties whose communications were intercepted had adequate notice of the interception." *In re Google Inc.*, 2013 WL 5423918, at *12 (N.D. Cal. Sept. 26, 2013). A website may only bind a user to terms "where the existence of the terms was reasonably communicated to the user." *Colgate v. JUUL Labs, Inc.*, 402 F. Supp. 3d 728, 764 (N.D. Cal. 2019).

The Ninth Circuit's decision in *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171 (9th Cir. 2014) controls here. In that case, the Ninth Circuit held, "where a website makes its terms of use available via a conspicuous hyperlink on every page of the website but otherwise provides no notice to users nor prompts them to take any affirmative action to demonstrate assent, even close proximity of the hyperlink to relevant buttons users must click on—without more—is insufficient to give rise to constructive notice." *Id.* at 1178-79 (internal citations omitted). The rule in *Nguyen* applies where a defendant argues disclosures in its Privacy Policy furnish a consent defense. *See Moreno v. San Francisco Bay Area Rapid Trans. Dist.*, 2017 WL 6387764, at *3 (N.D. Cal. Dec. 14, 2017) (following *Nguyen* and rejecting consent argument based on defendant's privacy policy); *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072-73 (N.D. Cal. 2016) ("*Opperman II*") (same).

Plaintiffs' allegations fall squarely within *Nguyen*. Plaintiffs allege the hyperlink to Noom's Privacy Policy on Noom's home page "was buried at the very bottom of the webpage in small, non-contrasting font (i.e., light grey against a white background) that was designed to be unobtrusive and easy to overlook." FAC ¶ 48. The hyperlink at the end of Noom's form is no better: it "is in the smallest text on the screen, not underlined, is not the typical color for a hyperlink, is not in all caps, and is surrounded by much more obvious and distracting features, such as the large orange 'See My Result' button." *Id.* at ¶ 51; *see also Colgate*, 402 F. Supp. 3d at 766

(hyperlinks insufficient where "[t]hey are not underlined [and] they are the same size as the sentence they are in."); *Maree v. Deutsche Lufthansa AG*, 2021 WL 267853, at *4 (C.D. Cal. Jan. 26, 2021) (hyperlinks insufficient where "Expedia.com's Terms of Use are not highlighted, underlined, in all capital letters, or displayed inside of a conspicuous and clickable box"). In its brief, FullStory does not take issue with any of these allegations.

Moreover, at no time are users ever told "*how* to accept the Privacy Policy." FAC ¶¶ 48-49. Indeed, there is no language suggesting that "by clicking 'See My Result,' users accept the Privacy Policy." *Id.* at ¶¶ 49, 51; *see also Nguyen*, 763 F.3d at 1179 (holding notice was insufficient where a website "provides no notice to users nor prompts them to take any affirmative action to demonstrate assent"); *Berman v. Freedom Financial Network, LLC*, 2020 WL 5210912, at *3 (N.D. Cal. Sept. 1, 2020) ("[T]here is no text that notifies users that they will be deemed to have agreed to these terms nor prompts them to take any affirmative action to demonstrate assent.") (internal quotations omitted); *Motley v. ContextLogic, Inc.*, 2018 WL 5906079, at *2 (N.D. Cal. Nov. 9, 2018) ("The screens also did not provide any notice that merely using the website would be deemed acceptance of the terms of service. The only thing ContextLogic's screens featured was an unadorned hyperlink to the terms of service."). Rather, users are only told that "[b]y submitting your email address, you may also receive email offers from us on Noom products and services."

Defendants do not even attempt to address these allegations, nor do they argue *how* users are even supposed to know that the Privacy Policy exists.[7] Accordingly, it would be reversible error to hold that Plaintiffs assented to or had notice of the Privacy Policy's terms under *Nguyen*.

3. The Privacy Policy Does Not Disclose The Wiretapping

Even assuming that Plaintiffs had notice of and consented to the Privacy Policy—and they did not—the Privacy Policy still does not disclose FullStory's wiretapping. "[C]onsent is only effective if the person alleging harm consented to the particular conduct, or to substantially the

[7] FullStory may attempt to argue on reply that the hyperlink to the Privacy Policy was sufficient to put users on notice. But this would be raising a new issue on reply, and outside the pleadings, which is improper. *Gadda*, 511 F.3d at 937 n.2 (9th Cir. 2007) ("It is well established that issues cannot be raised for the first time in a reply brief").

same conduct, and if the alleged tortfeasor did not exceed the scope of that consent." *Opperman II*, 205 F. Supp. 3d at 1072-73 (internal quotations omitted). If there is a dispute over the scope of a privacy policy or whether it adequately discloses the conduct at issue, then that is a question of fact that cannot be resolved on the pleadings. *See id.* (holding that "a reasonable jury could find that Yelp's Privacy Policy provisions do not explicitly address—and thus do not obtain knowing consent for—the uploading of a user's address book data for the purpose of finding friends who are already registered Yelp users"); *McCoy v. Alphabet, Inc.*, 2021 WL 405816, at *6 (N.D. Cal. Feb. 2, 2021) ("At the motion to dismiss stage, the Court is not prepared to rule that the Privacy Policy establishes an absolute bar to Plaintiff's claims."). Here, there are several reasons a jury could find that Noom's Privacy Policy does not disclose FullStory's wiretapping.

First, FullStory refers to a portion of Noom's Privacy Policy that states that "Noom and Noom's third-party service providers *may* use a variety of technologies that automatically (or passively) store or collect certain information whenever User visits or interacts with the Website ('Usage Information')." MTD at 15:3-7 (emphasis added).[8] "Usage Information" includes "the areas within Noom's Website and/or Mobile App that User visits and User's activities there." MTD at 15:7-8. But this disclaimer does not specify that users' every movement on a page is actively recorded in real-time. In other words, that Noom states it notes that a user visited a specific webpage is different than disclosing that Noom and FullStory are compiling a video of a user's every movement on that webpage. *See Opperman II*, 205 F. Supp. 3d at 1074 ("[I]t is unclear whether the language in the relevant Privacy Policy provisions even applies to the Friend Finder function at issue in this lawsuit."); *McCoy*, 2021 WL 405816, at *6 ("These statements may not be understood by a reasonable user to disclose collection of her usage information on an independent third-party app."). Indeed, as the FAC makes clear, "the extent of data collected by

[8] In making arguments about Noom's Privacy Policy, FullStory admits numerous times that it is a third party to Plaintiffs' communications with the Website. *See* MTD at 14:15-17 ("Noom's policy explicitly states that Noom and third parties may collect information from users of Noom's website, and that such information may be shared with *third parties like FullStory*.") (emphasis added); *id.* at 15:5-6 ("Noom and Noom's *third-party service providers* may use a variety of technologies that *automatically* (or passively) store or collect certain information.") (emphasis in original); *id.* at 15:14-17 ("The code is temporarily downloaded onto User's Device from Noom's web server and/or Mobile App or a *third party service provider*") (emphasis in original).

these services [like FullStory] **far exceeds user expectations**." FAC ¶ 55; *see also id.* ¶ 28 (noting FullStory is "unlike typical analytics services that provide aggregate statistics").

Second, the aforementioned section of the Privacy Policy states that Noom and third parties *may* collect Usage Information, not that they are definitively collecting such information. As a matter of law, "[t]hat the person communicating knows that the interceptor has the *capacity* to monitor the communication is insufficient to establish implied consent." *In re Google Inc.*, 2013 WL 5423918, at *12 (emphasis in original). Thus, the fact that Noom states it and third parties "*may*" collect Usage Information cannot support dismissal.

Third, FullStory refers to a portion of Noom's Privacy Policy that refers to "Embedded Scripts," which are defined as "programming code that is designed to collect information about User's interactions with the Website, Mobile App and Services, such as the links User clicks on." MTD at 15:11-17. But session replay technologies track *far* more information that "the links [a] User clicks on." *See* FAC ¶ 28 ("FullStory's code is not a cookie at all, much less a run-of-the-mill cookie. Common cookies that consumers might be familiar with do not engage in session recording."); *see also Campbell*, 77 F. Supp. 3d at 848 ("[A]ny consent with respect to the processing and sending of messages itself does not necessarily constitute consent to the specific practice alleged in this case—that is, the scanning of message content for use in targeted advertising."); *In re Google Inc.*, 2013 WL 5423918, at *13 (acceptance of activity "under a different set of circumstances for a different purpose" "does not establish explicit consent"). Accordingly, the Privacy Policy dilutes the meaning of embedded scripts—and thus, does not disclose the use of FullStory's technology—by refraining from revealing the full extent of the data collected by Session Replay. *Opperman II*, 205 F. Supp. 3d at 1074; *McCoy*, 2021 WL 405816, at *6. Further, the Privacy Policy again couches this disclaimer by stating that Noom or third parties "*may* use" these technologies. *In re Google Inc.*, 2013 WL 5423918, at *12.

Fourth, even if the "Embedded Scripts" section discloses the use of Fullstory's technology—and it does not—it misrepresents the nature of FullStory's technology. The Privacy Policy states that an embedded script "is active only while User is connected to the Website and/or

Mobile App, and is deactivated or deleted thereafter." FAC ¶ 54. But as FullStory admits on its website:

> If the user navigates away or closes their tab—which is normal behavior—FullStory bundles these events together into a "swan song" bundle, that is, a last ditch attempt to send the event data to FullStory before the page closes. **In some instances, the swan song isn't successful, so the data is stored locally in the user's browser, and the next time the user on that particular device visits the customer's site, the FullStory script will send the swan song data that weren't successfully sent on the user's last visit.**

Id. In other words, FullStory's code is not "is active only while User is connected to the Website and/or Mobile App," and is not "deactivated or deleted thereafter."

Finally, that Plaintiffs and FullStory can disagree about the scope of the Privacy Policy demonstrates that there is at least a question of fact as to what the Privacy Policy discloses not ripe for resolution on a motion to dismiss. *McCoy*, 2021 WL 405816, at *6.

III. PLAINTIFFS SUFFICIENTLY ALLEGE A CLAIM UNDER § 635

A. Plaintiffs Have Both A Private Right Of Action And Standing To Assert A Claim Under § 635

In two related arguments, FullStory argues Plaintiffs lack both a private right of action and standing to sue under § 635 "because … the mere manufacture, possession, or sale of an eavesdropping 'device' by a defendant … causes no injury to a person such as Plaintiff." MTD at 16:6-8. That is wrong.

FullStory's argument that Plaintiffs lack a private right of action contradicts the text of the statute. Section 635 imposes liability on "[*e*]*very person* who … *possesses* … or furnishes to another *any device* which is primarily or exclusively designed or intended for eavesdropping." Cal. Penal Code § 635 (emphasis added). Section 637.2 provides that "it is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or been threatened with actual damages." *Ion Equip. Corp. v. Nelson*, 110 Cal. App. 3d 868, 882 (1980); *see also* Cal. Penal Code § 637.2(b) (permitting any person to "bring an action to enjoin and restrain any violation of this chapter, *and may in the same action seek damages as provided by subdivision (a)*") (emphasis added). Thus, as shown in *Moosejaw*, there is a private right of action under § 635. *Moosejaw*,

2019 WL 5485330 at *3 (denying motion to dismiss § 635 claim). FullStory cites no contrary authority involving claims under CIPA.

Equally meritless is FullStory's argument Plaintiffs lack standing under *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016). MTD at 23:15-8. The court in *Moosejaw* rejected the same argument, based on the same authority, when it held that the plaintiff in that case had standing to assert a claim under § 635. *Moosejaw*, 2019 WL 5485330 at *1. The court explained that wiretapping is "not at all like the sort of 'bare procedural violation' that the Supreme Court has said [in *Spokeo*] would fall short of an Article III injury, and then held that plaintiff "alleged injuries traceable to Moosejaw's possession and use of the [internet monitoring] device." *Id.* at *1, *3. Moreover, the Ninth Circuit has held that wiretapping claims—including under CIPA—are beyond the scope of *Spokeo*. *See In re Facebook III*, 956 F.3d at 599 (holding "Plaintiffs have adequately alleged an invasion of a legally protected interest that is concrete and particularized" based on an alleged violation of CIPA); *see Romero v. Securus Techs., Inc.*, 216 F. Supp. 3d 1078, 1088 (S.D. Cal. 2016) (rejecting Defendants' same argument, holding that "[a] violation of CIPA involves much greater concrete and particularized harm than a technical violation of the Fair Credit Reporting Act ('FRCA'), the statute at issue in *Spokeo*.").

Standing is also supported by the Sixth Circuit's decision in *Luis v. Zang*, 833 F.3d 619 (6th Cir. 2016), which involved a claim under § 2512(b), a provision of the federal Wiretap Act that similarly prohibits the possession of wiretap devices. *See* 18 U.S.C. § 2512(b) (imposing liability on any person who "manufactures, assembles, [or] possesses" wiretapping devices). The *Luis* court first noted a split of authority as to whether mere possession alone could support a claim under § 2512(b), but ultimately concluded that possession, coupled with "knowledge" and "active[] involve[ment]" with the wiretapping, could support a claim. *Luis*, 833 F.3d at 636-37.

As in *Moosejaw* and *Luis*, Plaintiffs do not base their standing on the mere possession of a wiretapping device, but on FullStory's knowledge and active involvement in using that device to monitor his communications. *See* FAC, ¶¶ 1, 35-40, 43, 80.

B. Fullstory's Code Is A "Device" That Is "Primarily Or Exclusively" Designed For Eavesdropping

FullStory argues that "there is no reason to think that FullStory's code, which Noom is alleged to have embedded on its website, qualifies as a 'device' under the statute." MTD at 17:6-8. Then, relying solely on *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836 (N.D. Cal. 2017) ("*In re Facebook II*"), Defendants argue that even if it were a "device," Plaintiffs' allegations "do not support a plausible inference that the code is 'primarily or exclusively designed or intended for eavesdropping.'" MTD at 17:18-20. These arguments are meritless.[9] Plaintiffs allege that "FullStory's code is a 'device' that is 'primarily or exclusively designed' for eavesdropping. That is … FullStory's code is designed to gather PII, including keystrokes, mouse clicks, and other electronic communications." FAC ¶ 77; see also *id.* at ¶ 28 (noting that Fullstory's software is "intended for the recording and playback of individual browsing sessions, as if someone is looking over your shoulder"). Nothing more is required. *See Moosejaw*, 2019 WL 5485330, at *3 ("At the pleading stage, the Court must assume the truth of Revitch's allegation that NaviStone's code is a device … primarily or exclusively designed or intended for eavesdropping upon the communication of another.") (internal quotations omitted).

In any event, courts have rejected the same or similar arguments raised by Defendants because they rest on factual disputes about how the defendant's technology operates. *See In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1082 (N.D. Cal. 2015) ("[E]ven if the Defendants are factually correct that the communications at issue in this case were in transitory storage on Plaintiffs' mobile devices … it is not at all apparent why there was no 'captur[ing] or redirect[ing]' of these communications contemporaneous with their transmission."); *Campbell*, 77 F. Supp. 3d at 841 ("While Facebook may ultimately produce evidence showing that the messages were actually accessed while in storage, not during transmission, that issue is premature at this stage of the

[9] Notably, the portion of *In re Facebook II* quoted by Defendants concerned whether the plaintiffs "established that they ha[d] a reasonable expectation of privacy in the URLs of the pages they visit[ed]" – it was *not in the context of a Section 635 claim*. *In re Facebook II*, 263 F. Supp. 3d at 846. Accordingly, Defendants' argument that the software code at issue is "best understood as part of the routine internet functionality that makes digital commerce possible" is inapposite. MTD at 18:10-12. That argument also contradicts the allegations in the FAC. FAC ¶¶ 28, 34, 55.

case."); *cf. Moosejaw*, 2019 WL 5485330 at *3 (the question of whether defendant's internet tracking technology was a wiretap "device" under § 635 of CIPA is a question of fact).

Finally, FullStory argues that its software is not "intended for eavesdropping," but instead is intended "to help companies improve their websites." MTD at 18:6-7. This argument conflates what the software does with Defendants' purported motive for using that software. Few people wiretap simply for the sake of wiretapping: they will usually have a reason. If Defendants' argument could support dismissal, then any defendant could avoid liability by simply claiming they had a benevolent motive for the wiretapping. Motive, however, is irrelevant because it is not an element of a claim under § 635. Regardless, Plaintiffs allege that FullStory's software is far from routine, or a simple analytical software. FAC ¶¶ 28, 34, 55.

IV. PLAINTIFFS STATE A CLAIM FOR INVASION OF PRIVACY

FullStory argues that "Plaintiffs cannot plausibly allege a reasonable expectation of privacy in the information they provided" because they provided the information voluntarily. MTD at 19:3-5. Defendants also argue that even if Plaintiffs could allege a reasonable expectation of privacy, Plaintiffs do not allege that Defendants' conduct "constitutes an egregious breach of social norms." MTD at 19:15-16. These arguments fail for two reasons.

First, the arguments simply ignore Plaintiffs' allegations that "[u]sers are never told that their electronic communications are being wiretapped by FullStory." FAC ¶¶ 47, 53; *see also id.* at ¶ 56 ("Neither Plaintiffs nor any Class members consented to being wiretapped on [noom.com], nor to have their communications recorded and shared with FullStory."); Argument § II.C, *supra*. Plaintiffs also allege that FullStory's technology "far exceeds user expectations." FAC ¶ 55. Plaintiffs also allege that FullStory's software collects medical and health information (FAC ¶ 46), and the collection of intimate or sensitive personally identifiable information may amount to a highly offensive intrusion. *See*, *e.g.*, *Goodman v. HTC Am., Inc.*, 2012 WL 2412070, at *14-15 (W.D. Wash. June 26, 2012); *In re Vizio, Inc. Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1233 (C.D. Cal. 2017) ("*In re Vizio*") (same).

Second, in *In re Facebook III*, the Ninth Circuit reversed dismissal and rejected a similar argument, because "[t]he ultimate question of whether Facebook's tracking and collection practices

could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage." Even before *In re Facebook III*, numerous district courts had rejected similar arguments because they require a factual determination by the jury. *See In re Vizio*, 238 F. Supp. 3d at 1233 ("Considering the quantum and nature of the information collected, the purported failure to respect consumers' privacy choices, and the divergence from the standard industry practice, Plaintiffs plausibly allege Vizio's collection practices amount to a highly offensive intrusion."); *Opperman II,* 205 F. Supp. 3d at 1080 (holding that "there is a triable issue of fact regarding whether Yelp's upload of the Plaintiffs' address book data was highly offensive to a reasonable person"); *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125, 130 (3d Cir. 2015) (finding that plaintiffs stated a claims for violation of California's constitutional right to privacy where Google's conduct was "characterized by deceit and disregard … Google's alleged conduct was broad, touching untold millions of internet users; it was surreptitious, surfacing only because of the independent research of Mayer and the Wall Street Journal.").

CONCLUSION

For the foregoing reasons, the Court should deny Defendants' motion in its entirety. If the Court determines that the pleadings are deficient in any respect, Plaintiffs request leave to amend to cure any such deficiencies. *See Roney v. Miller*, 705 F. App'x 670, 671 (9th Cir. 2017) (lower court erred by denying leave to amend after dismissing amended complaint).

Dated: March 5, 2021

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Joel D. Smith*
Joel D. Smith

L. Timothy Fisher (State Bar No. 191626)
Joel D. Smith (State Bar No. 244902)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
jsmith@bursor.com

Attorneys for Plaintiffs